REMARKS/ARGUMENTS

No claims have been amended. Claims 23-44 have been added. No claims have been cancelled. Claims 1-44 remain pending in this application. Reexamination and reconsideration of the application as amended are respectfully requested.

Claim Rejections under 35 U.S.C. § 112, second paragraph:

Examiner has rejected Claims 2-3, 8-9, and 16-17 as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The terms "strong encryption" and "weak encryption" have been objected to in the Office Action. [Office Action, page 2]

The concept of "strong encryption" and "weak encryption" are well known to those skilled in the art. For example,

> By means of example, strongly encrypted data 103 may be distinguished from weakly encrypted data 103 merely by the size of the encryption key, the number of rounds performed by the block encryption cipher, or by the cipher itself. More particularly, a stream cipher is considered weaker than a block cipher because stream ciphers are not standardized and therefore have not received the same scrutiny as block ciphers. Another distinguishing factor in the robustness of encryption is the length of the key. A strong encryption key typically includes approximately one hundred twenty-eight bits while a weak encryption key typically only includes up to forty bits. A "bit" is typically the smallest unit of information in a computer system. The computer resources required to transform the data 103 by use of a large encryption key may be extensive and therefore operate slower than transformations that use a small encryption key. [Specification, page 14, lines 5-16]

The excerpt from the specification (page 14, lines 5-16), provides a standard for ascertaining strong encryption and weak encryption. In general, strong encryption implies that it would effectively be impossible to find the key within the effective lifetime of the secret. Weak encryption implies that the key could be found with a realistic amount of processing capacity and a reasonable amount of time. "During patent examination, the pending claims must be 'given their broadest reasonable interpretation consistent with the specification.'" In re Hyatt, 211 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000). [MPEP 2111] Therefore and given the description of strong encryption and weak encryption in the specification, Applicant respectfully requests that Examiner reconsider and withdraw the indefinite rejection.

Claim Rejections under 35 U.S.C. § 102(e)

Claims 1-4, 7-10, and 15-18 have been rejected as being anticipated by Mitty et al. US Patent No. 6,145,079 ("Mitty"). "Mitty teaches a data element being statically encrypted with a static key, a data element being dynamically encrypted with a dynamic key, and a data element being decrypted with a dynamic key and a static key." [Col 12, line 61 - Col. 13 line 17] "Mitty teaches encryption with a static key being strong encryption" [Col. 8 lines 48-51] "Mitty teaches encryption with a dynamic key being weak encryption" [Col 12, lines 14-23] Regarding the claims 4, 10, and 18, Mitty teaches encrypting a static key on a first computer system, encrypting a dynamic key on a second computer system, and decrypting the static key and the dynamic key. [Office Action, page 3]

Mitty teaches an electronic messaging system, requiring a non-streamed (non-chunked) environment with the entire data contents, envelope and contents, available. [Mitty, Abstract] "There is a need in the art for an electronic message system that provides privacy, authentication of participants, and non-repudiation." [Mitty, Col. 2, lines 1-3] Mitty teaches secure electronic transmissions that are applied to "packages" that include the entire data contents.

> "Using techniques described below, sender 105 transmits a "package" to a trusted intermediary 115 via potentially non-secure network 110, such as the Internet." [Mitty, Col. 6, lines 26-27] "In short, both the original and new version of the package have an inner and outer "digital envelope." These digital envelopes are instances of envelopedData, and information they contain enable the system to provide privacy, authentication, and non-repudiation." [Mitty, Col 6, lines 57-61]

In contrast, Applicants' invention operates in either a chunked or non-chunked environment thereby improving performance of the transmission of encrypted data. It would not have been obvious to one skilled in the art to attempt to extend the teachings of Mitty from an electronic messaging system supporting non-chunked data, to a system supporting video stream data or chunk data. Applicants' invention enhances performance of encryption and decryption of data elements by operating on chunked or non-chunked data. For example,

> The data 103 used and created on the data server 102 may be stored in computer-readable media data storage 116. The dynamically encrypted data 114 is typically not

> stored on permanent storage, such as computer disks. For example, the dynamically encrypted data 114 may be stored in computer memory. Further, the dynamically encrypted data 114 may be partitioned into chunks and each chunk may be processed with the use of computer memory thereby eliminating storage during the operation of the present invention. (Specification, page 11, lines 5-11)

Further, it would not have been obvious to one skilled in the art to extend the teachings of Mitty that require the entire data contents to be used in the encryption and decryption process, to a chunked environment that does not require availability of all the contents contained within an envelope. More particularly, the focus of Mitty is an electronic messaging system, which is not similar to the focus of Applicant's invention that operates in either a chunked or a non-chunked, streamed data, environment. For example, Applicants' invention enables such a flexible, high-performance solution that operates with some personalized or dynamic features typically associated with chunked dynamically encrypted data. For all the foregoing reasons, Applicants respectfully request allowance of independent Claims 1, 7, and 15; and dependent claims 2 - 4, 8 - 10, and 16 - 18.

Claim Rejections under 35 U.S.C. § 103(a)

Examiner has rejected Claim 5 as being unpatentable over Mitty et al. "With regards to claim 5, Mitty fails to teach the second computer being untrusted. Examiner contends that untrusted computers are well known in the art and it would have been obvious to a person of ordinary skill in the art to allow Mitty's system to work with untrusted computers because it offers the advantage of allowing interoperability with a far wider range of networks and systems." [Office Action, page 4]

> To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. [MPEP Section 2142]

Examiner has indicated that the motivation for allowing Mitty's system to work with untrusted computers is because it offers an advantage of allowing interoperability with a far wider range of networks and systems. Mitty requires the use of a trusted intermediary. [Mitty, Col 2, line 12] Applicant's invention does not require a trusted intermediary, working on streamed, or chunked data, with either a trusted or an untrusted computer system. It would not have been obvious to one skilled in the art to use an untrusted computer as is taught by Applicants' invention, because the techniques of Applicants' invention were not known at the time the invention was conceived. Part of the problem in the past was that such features required and relied upon a trusted computer intermediary. Therefore, an aspect of the novelty of Applicants' invention is that it operates on chunked or non-chunked data and does not require a trusted computer system. Applicants' Claim 5, is not obvious in view of Mitty.

Examiner is respectfully reminded that,

> The requirement 'at the time the invention was made' is to avoid impermissible hindsight ' . . . 'It is difficult but necessary that the decisionmaker forget what he or she has been taught. . . about the claimed invention and cast the mind back to the time the invention was made (often as here many years), to occupy the mind of one skilled in the art who is presented only with the references, and who is normally guided by the then-accepted wisdom in the art.' [MPEP Section s2141.01.III]

With respect to Claim 5, Applicants' invention does not require a trusted intermediary. It would not have been obvious to one skilled in the art at the time Applicants' invention was created to apply the teachings of Mitty to Applicant's invention. Reconsideration and allowance of Claim 5 is respectfully requested.

Claims 6, 11, and 19 are rejected as being unpatentable over Mitty in view of Bailey III US Patent No. 5,659,614 ("Bailey"). Mitty teaches Claims 6, 11, 19 with the exception that Mitty, "fails to teach the data element being decrypted by the same dynamic key on a second computer system." [Office Action, Page 5] "Bailey teaches the data element being decrypted with the static key and the dynamic key on a second computer system [Bailey, column 6 lines 9-21, column 18 lines 53-55] [Office Action, Page 5]

Claims 6, 11, and 19 are dependent, respectively, on independent Claims 1, 7, and 15. For all the reasons put forth with respect to independent Claims 1, 7, and 15, and Claims 1-4, Applicant claims that Claims 6, 11, and 19 are not obvious over Mitty. Further, Bailey is focused on decryption at a backup site and is related to file data, not chunked data. "A method and system for prioritizing, securing, and reducing the amount of data transmitted and stored during the creation of a backup copy of file data." [Bailey, Abstract] It would not have been obvious to one skilled in the art to use the techniques of Bailey that are focused on backup techniques for file data, for the purpose of rendering obvious Applicants' invention. Further, Bailey requires a data security card for additional numbers to serve as keys (Col. 18, lines 30-44) and this technique is not similar the techniques of Applicants' invention. For all the reasons put forth, Applicants respectfully request that that Claims 6, 11, and 19 be allowed.

Claims 12-13 and 20-21 have been rejected as being unpatentable over Mitty in view of Koopman Jr. et al. RE36,181. "Koopman teaches pseudorandom number generation system with cryptographic authentication." [Office Action, Page 5] "Mitty teaches the determination of whether a transmission failed (Mitty Col. 6- lines 30-56, confirmation messages) but fails to teach the repairing of the data element without retransmission." But Koopman teaches the missing element [Koopman Col. 16, 44-56] [Office Action, Page 5]

While Koopman focuses on automobile door lock receiver ("keychain fob") encryption technology Applicants' invention teaches state recoverability of encryption systems, and it would not have been obvious to one skilled in the art to use the techniques of Koopman to render Applicants' invention obvious. For example, Applicants' invention teaches recovery of an unreliable channel as follows,

> Third, if an unreliable channel is used, the data decryption method 504 requires a way to recover the state, "s," 604 in order to decrypt the data 103 that follows the transmission loss. That is, the data decryption method 504 includes state recoverability information in the form of the state, "s," 604. The method of saving the state, "s," 604 is described with reference to elements 525 and 527 in Figure 5B. The method of extracting the state, "s," 604 is described with reference to element 568 in Figure 5C.

> Fourth, if the static encryption requires maintenance of the state, "s," 604 to enable decryption, either the transmission channel between the encrypting computer system and the decrypting computer system should be reliable or the method of data decryption 504 should enable recovery of the state, "s," 604. To enable recoverability, the payload buffer size, "p," 606 is typically the size of the data 103 presented in a buffer plus the size of the state, "s," 604 for encryption with a static key 108. [Specification, page 19, lines 6 – 19]

In contrast, the error correction code detection relied on by Koopman [Col. 16, lines 43-56] is not relied on by Applicants' teachings of repairing a data element without retransmission of the data [Specification, Claims 12-13 and 20-21]. Koopman relies on error correction that is a "single error" correction, ". . . correcting any single error which can be fixed". [Koopman, Col 16, lines 47-48] It would not have been obvious to one skilled in the art to use the techniques of Koopman that are directed to keychain fob encryption and rely on single error correction code, and extend them to the techniques of Applicants' invention that recovers from error on any chunked or non-chunked data element. Applicants respectfully request that that Claims 12-13 and 20-21 be allowed.

Claims 14 and 22 have been rejected by Mitty in view of Koopman, and further in view of Bailey. The Examiner has indicated that Mitty, ". . . fails to teach the repairing of the data element without retransmission". [Office Action, Page 6]

For all the reasons put forth with respect to Claims 12-13 and 20-21, Applicants assert that Claims 14 and 22 should be allowed. The Examiner has not put forth any specific arguments with respect to Bailey. Bailey teaches techniques of backup on data files. Appplicants' invention applies to chunked and non-chunked data and is not rendered obvious by Bailey's techniques of backup of data files.

New Claims

Further, Applicants have added Claims 23-44 to distinguish that the present invention operates both in an environment of chunked or non-chunked data, and in an environment including only chunked data. Claims 23-44 teach Applicants' invention in a chunked environment and do not claim new matter. "Further, the dynamically encrypted data 114 may be partitioned into chunks and each chunk may be processed with the use of computer memory thereby eliminating storage during

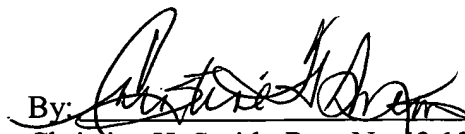
the operation of the present invention." [Specification, page 11, lines 9-11] For all the reasons put forth above, allowance of Claims 23-44 is respectfully requested.

Conclusion

For all the above reasons, Applicant submits that the pending Claims 1-44 are patentable over the art of record. Applicants have added Claims 23-44. Please charge Deposit Account No. 09-0460 for any additional fees that are required.

Applicants therefore respectfully request that the Examiner reconsider all currently outstanding objections and rejections and that they be withdrawn. It is believed that a full and complete response has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this Application, the Examiner is invited to telephone the undersigned at the number provided. Prompt and favorable consideration of this Response is hereby solicited.

Respectfully submitted,
Amini et al

By: 

Christine H. Smith, Reg. No 43,133
Attorney/Agent for Applicant(s)
International Business Machines Corporation
Intellectual Property Law
555 Bailey Avenue, J46A/G469
San Jose, CA 95141-9989
Telephone: (408) 463-5671

Date: January 13, 2005